ПРОБЛЕМЫ УМНЫХ ГОРОДОВ И УСТОЙЧИВОЕ РАЗВИТИЕ ТЕРРИТОРИЙ

ПРОГНОЗИРОВАНИЕ ИНТЕНСИВНОСТИ КИБЕРАТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

[1,2]Краковский Ю. М., [3]Лузгин А. Н.

[1]Иркутский государственный университет путей сообщения, Иркутск
[2]Иркутский государственный университет, Иркутск, Россия
[3]Администрации города Иркутска, Россия

e-mail: 79149267772@yandex.ru alexln@mail.ru

Аннотация. В нормативных документах последних лет в сфере информационной безопасности уделяется большое внимание информационным системам критических инфраструктур. Это, в свою очередь, обосновывает необходимость научных исследований по разработке новых методов защиты от кибератак на такие информационные системы. Для этой задачи рекомендуется интервальное прогнозирование на основе вероятностной нейронной сети с динамическим обновлением параметра сглаживания. В качестве эталонов для сравнения результатов интервального прогнозирования были выбраны наивная байесовская модель и вероятностная кластерная модель.

Ключевые слова: Интервальное прогнозирование, кибератаки, критическая инфраструктура, информационные системы, вероятностная нейронная модель, вероятностная кластерная модель

THE CYBERATTACK INTENSITY FORECASTING TO INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURES

Y. M. Krakovsky[1,2], A. N. Luzgin[3]

[1]Irkutsk State Transport University, Irkutsk, Russia
[2]Irkutsk State University, Irkutsk, Russia
[3]Administration of Irkutsk city, Irkutsk, Russia

e-mail: 79149267772@yandex.ru alexln@mail.ru

Abstract. In regulatory documents of recent years in the field of information security, much attention is paid to information systems of critical infrastructures. This, in turn, justifies the need for scientific research on the development of new methods of protection against cyberattacks on such information systems. For this task, interval forecasting is recommended based on a probabilistic neural network with dynamic updating of the smoothing parameter. As benchmarks for comparing the interval forecasting results, the naive Bayesian model and the probabilistic cluster model were chosen.

Key words: Interval forecasting, cyberattacks, critical infrastructure, information systems, probabilistic neural model, probabilistic cluster model.

1. Введение

В последние годы в Российской Федерации и в мире большое внимание уделяется безопасности критических инфраструктур. В соответствии с принятым в 2017 году федеральным законом «О безопасности критической информационной инфраструктуры Российской федерации» [1], информационные системы (ИС) являются важными

объектами защиты. Эти объекты попадают под Указ Президента РФ от 15.01.2013 №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». В развитие этого указа, в декабре 2014 года Президентом страны была утверждена концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В соответствии с этой концепцией основными функциями системы являются: выявление признаков проведения компьютерных атак, определение их источников и другой связанной информации, прогнозирование ситуации в области обеспечения информационной безопасности РФ, сбор и анализ информации о компьютерных атаках в отношении информационных ресурсов РФ, осуществление мероприятий по оперативному реагированию на атаки и ликвидации их последствий [2].

В 2016 году была принята «Доктрина информационной безопасности Российской Федерации», где отмечается, что «состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом кибератак на объекты критической информационной инфраструктуры» [3]. В федеральном законе «О безопасности критической информационной инфраструктуры Российской федерации» [1] отмечается, что устанавливается обязательное требование о внедрении государственной системы обнаружения, предупреждения и ликвидации последствий кибератак на ИС критических инфраструктур. Это еще раз подтверждает значимость и актуальность вопросов кибербезопасности ИС критических инфраструктур для Российской Федерации. Таким образом, научные исследования по разработке новых методов защиты от кибератак ИС критических инфраструктур являются актуальными и необходимыми.

Одним из перспективных направлений исследований для решения задачи защиты от кибератак на ИС является создание методов прогнозирования их интенсивности посредством машинного обучения [4, 5]. Отметим, что под интенсивностью кибератак понимается суммарное число этих атак в единицу времени. В случае получения прогноза о том, что интенсивность кибератак на ИС превышает некоторую заранее заданную величину, могут приниматься дополнительные меры защиты, включая, например, проведение более глубокого интеллектуального анализа трафика. Отметим, что в ФЗ «О безопасности критической информационной инфраструктуры Российской федерации», равно как и в «Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» подчеркивается необходимость в осуществлении прогнозов в сфере кибербезопасности. Таким образом, при создании системы защиты ИС для противодействия кибератакам, кроме реализации системы управления информационными рисками, их информационного аудита и анализа, необходимо уделять внимание прогнозированию интенсивности кибератак [6].

В последние годы наблюдается возрастающий интерес исследователей к вероятностному прогнозированию кибератак [7, 8]. Это можно объяснить тем, что вероятностные прогнозы позволяют получать не только прогнозы непосредственно будущих событий, но и оценки их вероятностей.

Разновидностью вероятностного прогнозирования является интервальное прогнозирование (ИП) [9–11]. Суть этого прогнозирования заключается в

прогнозировании одного из двух заранее заданных интервалов, в котором будет находиться будущее значение показателя на основе оценок вероятностей этих событий. Разделительная граница интервалов задается расчетным способом, исходя из статистических характеристик этого показателя.

В данной работе для прогнозирования интенсивности кибератак на ИС рекомендуется ИП на основе вероятностной нейронной сети с динамическим обновлением параметра сглаживания (ВНМ) [10, 11]. В качестве эталона для сравнения результатов ИП была выбрана наивная байесовская модель (НБМ) [12] и вероятностная кластерная модель (ВКМ) [13].

2. Описание и формализация показателя интенсивности кибератак

Учитывая, что информация об интенсивности кибератак на объекты информатизации транспорта носит конфиденциальный характер, в качестве такого показателя в работе рассматривается количество кибератак за сутки, которые происходили с 1998 по 2015 год в Южной Кореи (CAI) [14]. Данный показатель был выбран по причине своей общедоступности и большого объёма исходной выборки, подходящей для построения любых моделей машинного обучения с целью ИП. С другой стороны, выбранный показатель является нестационарным по параметру положения и параметру масштаба, что подчеркивает его непростую статистическую «природу» [10]. Тем самым, если этот показатель покажет хорошие результаты ИП интенсивности кибератак, то мы можем с большей уверенностью сделать подобные выводы применительно к объектам информатизации транспорта.

Формализуем этот показатель в виде временного ряда:

$$\boldsymbol{z} = \{z_t : t \in \boldsymbol{t}\} \quad (1)$$

Здесь z_t – значения показателя в дискретные моменты времени, где t принимает значения из множества $t \in$ t, t = $\{1,\dots n\}$, а n – количество (объем) значений показателя. Для выбранного показателя n = 1552.

Пусть $[z_{\min}; z_{\max}]$ – условный диапазон возможных значений показателя (1), тогда z_α – порог интенсивности кибератак ($z_{\min} \le z_\alpha \le z_{\max}$). Порог интенсивности кибератак z_α – это такое значение, для которого вероятность того, что $z_t \le z_\alpha$ равна α. Таким образом, z_α – это квантиль функции распределения вероятностей показателя (1) при заданной вероятности α.

Далее предлагается выполнить следующее полностью обратимое преобразование исходного показателя (1):

$$\boldsymbol{q} = log(\boldsymbol{z} + 1) - log(z_\alpha + 1) = \{q_t : t \in \boldsymbol{t}\}. \quad (2)$$

Здесь q_t – значения показателя в дискретные моменты времени, где t принимает значения из множества $t \in$ t, t = $\{1,\dots n\}$, а n – количество (объем) значений показателя (2), z_α – порог интенсивности кибератак.

Такое преобразование полезно по нескольким причинам:

- значения исходного показателя (1) лежат в очень широком диапазоне и некоторые (экстремальные) значения существенно превышают остальные. Логарифмирование помогает улучшить визуальную работу с такими данными и их графиками;
- показатель (2) содержит как положительные, так и отрицательные значения, в отличие от показателя (1). Некоторые модели прогнозирования (в том числе ВНМ)

«чувствительны» к знаку предикторов и демонстрируют лучшую точность ИП после проведения подобных преобразований;

– эквивалентом z_α для показателя (2) всегда является нулевое значение. То есть распределение положительных и отрицательных величин относительно z_α для показателя (1) и относительно 0 для полученного показателя (2) идентичны и это позволяет немного упростить формализацию ИП показателя (2) без искажения сущности и интерпретации получаемых результатов.

На рисунке 1 приведен график полученного показателя (2).

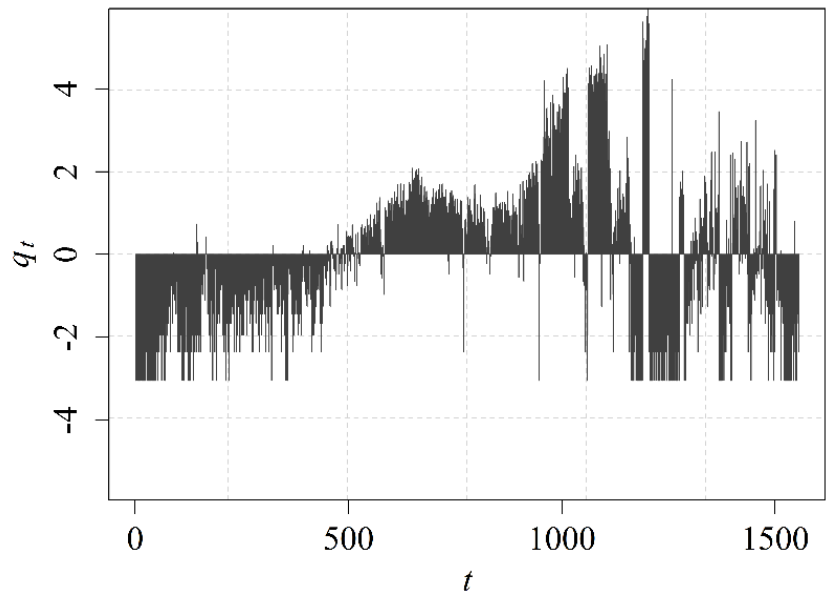

Рис. 1. График показателя q (2), полученный при α = 0,5

Таким образом следует отметить, что преобразование показателя (1) в показатель (2) есть неотъемлемая составляющая процесса осуществления ИП.

Для получения некоторых статистических характеристик данного показателя был определён его класс, методом, описанном в работе [10]. Указанный показатель является показателем первого класса, нестационарным по параметру положения и масштаба, что свидетельствует о его непростой статистической «природе» среди показателей других классов [9, 10].

3. Формализация интервального прогнозирования интенсивности кибератак

Пусть $[q_{\min};\ q_{\max}]$ – условный диапазон возможных значений показателя (2). Создадим два интервала:

$$I^- = (q_{min}; 0], I^+ = (0; q_{max}) \quad (3)$$

При ИП в момент времени $t = n$ необходимо определить, в каком интервале (3) будет находиться будущее (неизвестное) значение q_{t+p} на основе оценок вероятностей ρ_{t+p}^+ и ρ_{t+p}^-, где $p = 1, \dots, r$ – время упреждения; ρ_{t+p}^+– вероятность того, что будущее значение $q_{t+p} \in I^+$, ρ_{t+p}^- – вероятность того, что будущее значение $q_{t+p} \in I^-$; $\rho_{t+p}^+ + \rho_{t+p}^- = 1$.

Пусть $\tilde{\rho}_{t+p}^{+}$ и $\tilde{\rho}_{t+p}^{-}$ оценки соответствующих неизвестных вероятностей ρ_{t+p}^{+} и ρ_{t+p}^{-}. ИП проводится по правилу: будущее значение $q_{t+p} \in I^{+}$, если $\tilde{\rho}_{t+p}^{+} > \tilde{\rho}_{t+p}^{-}$; будущее значение $q_{t+p} \in I^{-}$, если $\tilde{\rho}_{t+p}^{+} \leq \tilde{\rho}_{t+p}^{-}$.

4. Формализация обучающей выборки вероятностных моделей

Необходимо рассмотреть некоторые особенности формирования обучающей выборки для осуществления ИП.

Пусть при $t = n$ имеется последовательность значений $q_{t-f+1}, \dots, q_t$ количеством f. Сформируем матрицу-строку $\mathbf{h} = \left(q_{t-f+1}, \dots, q_t\right)$ размером $1 \times f$.

Пусть имеется зависимая переменная-признак (называемая также откликом) y_{t+p} истинное значение которой неизвестно и которая может принимать только два возможных значения: $y_{t+p} = 1$, если $q_{t+p} \in I^{+}$ и $y_{t+p} = -1$, если $q_{t+p} \in I^{-}$.

При осуществлении ИП, используя h, требуется выполнить прогноз отклика y_{t+p} на основе оценок вероятностей того, что $q_{t+p} \in I^{+}$ и $q_{t+p} \in I^{-}$.

Используя значения показателя (2) для $t = 1, \dots, m$, где $m = n - f - p + 1$ (это значение выбрано так, чтобы можно было рассчитать значения всех откликов по предыстории показателя), построим обучающее множество:

$$\boldsymbol{x} = \begin{pmatrix} q_1 & \cdots & q_{1+f-1} \\ & \cdots & \\ q_m & \cdots & q_{m+f-1} \end{pmatrix}, \boldsymbol{y} = (y_1, .., y_m) \qquad (4)$$

Здесь **x** – матрица предикторов размером $m \times f$, где индекс каждого предиктора указывает на позицию соответствующего элемента в (2); **y** – матрица-строка откликов размером $1 \times m$ (эти отклики рассчитываются по предыстории показателя); m – число «обучающих» примеров или объектов.

Каждой строке матрицы x соответствует отклик матрицы-строки **y** (4). Используя обучающее множество (4), можно построить и обучить некоторую модель прогнозирования, а также осуществить ИП, используя h. Часто матрица предикторов хиспользуется не в чистом виде, а в преобразованном. Например, для ВНМ каждая строка матрицы x преобразуется так, чтобы сумма квадратов значений каждой строки была равна единице. Для БНМ это делать необязательно.

5. Общий алгоритм интервального прогнозирования интенсивности кибератак

Алгоритм ИП в общем виде состоит из следующих этапов:

- подготовка исходных данных: **z** (1);
- задание параметра: α;
- построение кусочно-линейной функции распределения вероятностей показателя **z** (1) и определение z_α для заданного α.
- преобразование **z** (1) в **q** (2).
- задание параметров: *p, f*;
- формирование обучающей выборки (4);
- выбор модели прогнозирования и задание ее параметров (значения параметров могут быть оптимизированы по обучающей выборке, например, методом кросс-валидации [15]);
- осуществление ИП.

Таким образом, алгоритм имеет три параметра: α – вероятность, с которой интенсивность кибератак будет ниже порогового уровня интенсивности кибератак z_α; p – время упреждения; f – размерность обучающих векторов-предикторов.

6. Результаты интервального прогнозирования интенсивности кибератак и перспективы их практического применения

Для анализа результатов ИП интенсивности кибератак нами использовалось несколько величин. Рассмотрим их подробнее и аргументируем выбор каждой из них.

Прежде всего, нас интересует точность, с которой осуществляется прогнозирование событий $q_{t+p} \in I^+$. В самом деле, при получении такого прогноза, необходимо принять дополнительные меры защиты от возрастающих кибератак. Чем точнее такие прогнозы, тем реже будут ошибочно приниматься дополнительные меры противодействия кибератакам (ложные срабатывания). Чем меньше ложных срабатываний, тем эффективнее будет работать система защиты от кибератак. Для оценки точности таких прогнозов предлагается использовать величину:

$$pr^+ = l^+/u^+ \quad (5)$$

где pr^+ – оценка точности прогнозирования событий $q_{t+p} \in I^+$, l^+ – число оправдавшихся прогнозов того, что $q_{t+p} \in I^+$, u^+ – общее число сделанных прогнозов того, что $q_{t+p} \in I^+$, $0 \le pr^+ \le 1$.

Также нас интересует точность, с которой осуществляется прогнозирование событий $q_{t+p} \in I^-$. Здесь, при получении прогноза о том, что $q_{t+p} \in I^-$, система защиты от кибератак продолжает функционировать в штатном режиме. Чем точнее такие прогнозы, тем реже будут возникать ситуации, когда по факту требовалось принятие дополнительных мер защиты от кибератак, но этого не было сделано. Это также влияет на эффективность системы защиты от кибератак. Для оценки соответствующей точности таких прогнозов использовалась величина:

$$pr^- = l^-/u^- \quad (6)$$

где pr^- – оценка точности прогнозирования событий $q_{t+p} \in I^-$, l^- – число оправдавшихся прогнозов того, что $q_{t+p} \in I^-$, u^-– общее число сделанных прогнозов того, что $q_{t+p} \in I^-$, $0 \le pr^- \le 1$.

Таким образом, чем больше значения pr^+ и pr^- – тем лучше. Отметим, что модель прогнозирования должна как можно точнее прогнозировать оба варианта событий: $q_{t+p} \in I^+$ и $q_{t+p} \in I^-$. Например, модель, которая даёт результат $pr^+ = 0.75$ и $pr^- = 0.80$, предпочтительнее той, которая даёт результат $pr^+ = 0.55$ и $pr^- = 0.95$. Это позволяет определить итоговую величину, характеризующую точность ИП выбранной модели:

$$pr = min(pr^+, pr^-). \quad (7)$$

Здесь pr^+ – оценка точности прогнозирования событий $q_{t+p} \in I^+$ (5), pr^- – оценка точности прогнозирования событий $q_{t+p} \in I^-$ (6). Чем больше значение pr (7), тем точнее ИП.

Тестирование выбранных моделей проводилось следующим образом. Обучающее множество (4) разбивалось на две части. Первая часть, которая включала в себя четные строки матрицы x и элементы y, использовалась для обучения моделей, тогда вторая часть с нечетными строками матрицы x и элементами y использовалась для получения

прогнозов. Затем наоборот, вторая часть использовалась для обучения моделей, а первая часть для получения прогнозов. После этого оценивались величины (5–7). Иными словами, величины (5–7) оценивались методом кросс-валидации по двум блокам (2-fold cross validation) [15].

Оценки величин (5-7) проводились для различных значений α от 0,20 до 0,80 с шагом 0,1. Параметр p во всех случаях был задан 1. При фиксированном значении α осуществлялся последовательный перебор значений параметра f от 1 до 10 (этот параметр общий для ВНМ и НБМ). При этом для НБМ для каждого нового значения f проводился перебор значений параметра сглаживания непараметрического восстановления плотностей вероятностей предикторов от 0,1 до 1 с шагом 0,1. Среди всех полученных оценок (7) выбиралась такая модель в своем классе, для которой значение (7) было максимально. Все алгоритмы и расчеты были реализованы на языке R [16–18].

В таблице 1 приведены полученные результаты.

Таблица 1

Результаты расчетов

Параметр, α	**Порог,** z_α	**ВКМ,** *pr*	**ВНМ,** *pr*	**НБМ,** *pr*
0.2	3	0.66	**0.75**	0.60
0.3	6	0.75	**0.77**	0.70
0.4	11	0.83	**0.84**	0.81
0.5	20	0.88	**0.88**	0.88
0.6	35	0.86	**0.88**	0.83
0.7	55	0.80	**0.81**	0.75
0.8	79	0.74	**0.79**	0.77

Как следует из приведенных результатов, по сравнению с ВКМ и НБМ, ВНМ является более точной и приемлемой. При этом наблюдается следующая общая тенденция для выбранных моделей: наибольшая точность наблюдается в середине значений параметра α, но и для других значений точность остается приемлемой. На практике выбор значения параметра α может осуществляться экспертным путем. Следует отметить, что диапазон α от 0,20 до 0,80 является вполне достаточным для решения практических задач. Задавать большие или меньшие значения α нецелесообразно. К тому же это приведет к серьезному «дисбалансу» обучающей выборки и, как следствие, результаты ИП могут быть нестабильными и неадекватными.

Возможны дополнительные меры противодействия кибератакам, которые должны применяться не при первом попадании будущего значения в интервал I^+, а после некоторого числа попаданий. В этом направлении необходимы дополнительные исследования.

7. Заключение

Как следует из результатов данной работы, интервальное прогнозирование интенсивности кибератак на объекты информатизации критических инфраструктур актуальной и важной практической задачей. Проведенные экспериментальные исследования интервального прогнозирования интенсивности кибератак посредством вероятностной нейронной сети с динамическим обновлением параметра сглаживания, вероятностной кластерной модели и наивной байесовской модели показали, что

предложенный подход на основе нейронной сети имеет лучшую точность интервального прогнозирования выбранного показателя интенсивности кибератак.

Учитывая, что информация об интенсивности кибератак на объекты информатизации транспорта носит конфиденциальный характер, в качестве такого показателя в работе рассматривалось количество кибератак за сутки, которые происходили с 1998 по 2015 год в Южной Кореи (CAI) [14].

Данный показатель был выбран по причине своей общедоступности и большого объёма исходной выборки, подходящей для построения любых моделей машинного обучения с целью ИП. С другой стороны, выбранный показатель является нестационарным по параметру положения и параметру масштаба, что подчеркивает его непростую статистическую «природу». Так как этот показатель показал хорошие результаты интервального прогнозирования интенсивности кибератак, то мы делаем подобные выводы применительно к объектам информатизации транспорта.

Список литературы

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской федерации» от 26.07.2017 №187-ФЗ.

2. Выписка из концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской федерации, утвержденной Президентом Российской Федерации от 12.12.2014 № К1274.

3. Указ Президента РФ «Об утверждении доктрины информационной безопасности Российской Федерации» от 5.12.2016 №646.

4. Петренко С.А Концепция раннего распознавания и предупреждения компьютерного нападения / С.А. Петренко, А.С. Петренко // Материалы всероссийской научно-практической конференции «Информационные системы и технологии в моделировании и управлении». – 2016. – С. 82-86.

5. Петренко С.А. Национальная система раннего предупреждения о компьютерном нападении / С.А. Петренко, Д.Д. Ступин. – Иннополис: Издательский Дом «Афина». – 2017. – 440 с.

6. Gandotra E. Computational Techniques for Predicting Cyber Threats / E. Gandotra, D. Bansal, S. Sofat // Procceediongs of Intelligent Computing, Communication and Devices. – 2015. – P. 247–253.

7. Zhan Z. Predicting cyber-attack rates with extreme values / Z. Zhan, M. Xu, S. Xu. // IEEE Transactions on Information Forensics and Security . – 2015. – №. 10 (8). – P. 1666–1677.

8. Werner G. Time series forecasting of cyber-attack intensity / G. Werner, S. Yang, K. McConky // Proceedings of the 12th Annual Conference on Cyber and Information Security. – 2017. – P. 224–240.

9. Краковский Ю.М. Прикладные аспекты применения интервального прогнозирования в системном анализе / Ю.М. Краковский, А.Н. Лузгин А.Н. // Современные технологии. Системный анализ. Моделирование. – 2017. – № 2 (54). – С. 115 – 121.

10. Kargapoltsev S.K. Nonparametric classification of technical condition parameters based on shift and scale tests / S.K. Kargapoltsev, Y.M. Krakovsky, A.N. Luzgin // 2017 International Conference on Industrial Engineering, Applications and Manufacturing. – 2017. – P.1–5.

11. Kargapoltsev S.K. A dynamic updating algorithm of smoothing parameter values of probabilistic neural networks / S.K. Kargapoltsev, Y.M. Krakovsky, A.V. Lukyanov, A.N. Luzgin // Far East Journal of Electronics and Communications. – 2017. – vol. 17. – №. 4. – P. 909–914.

12. Ethem A. Introduction to Machine Learning: Massachusetts Institute of Technology. – The MIT Press Cambridge. – 2014. – 616 p.

13. Krakovsky Y.M. Robust interval forecasting algorithm based on a probabilistic cluster model / Y.M. Krakovsky, A.N. Luzgin // Journal of statistical computation and Simulation. – 2018. – vol. 88. – no. 12. – pp. 2309–2324.

14. Han L. WHAP: Web-hacking profiling using Case-Based Reasoning / L. Han, Ch. Han, R. Kang, I. Kwak, A. Mohaisen, H. Kim // 2016 IEEE Conference on Communications and Network Security. – 2016. – P.344–345.

15. Browne M. Cross-validation methods / M. Browne // Journal of mathematical psychology. –2000. – vol. 44. –P.108–132.

16. The R Project for Statistical Computing. Режим доступа: https://www.r-project.org.

17. Краковский Ю.М. Интервальное прогнозирование интенсивности кибератак на объекты критической информационной инфраструктуры / Ю.М. Краковский, Б.В. Курчинский, А.Н. Лузгин // Доклады ТУСУР. – 2018. – Т. 21. – №1. – С.71–79.

18. Краковский Ю.Мю Программное обеспечения интервального прогнозирования нестационарных динамических показателей / Ю.М. Краковский, А.Н. Лузгин // Вестник ИрГТУ. – 2015. – Т.1. – № 4. – С.12–16.